Remarks

Claims 1-9, 13-21, and 25-33 are pending but stand rejected. . Claims 1-7, 13-19, and 25-33 have been amended. Claims 10-12, 22-24, and 34-36 were previously cancelled. In view of the amendments and following remarks, the applicants respectfully ask for the Examiner's thoughtful reconsideration.

AMENDMENTS

Each independent claim has been amended to recite (a) issuing a first security key that is indicative of greater printing resource authorization to client computers that are members of a predetermined policy domain and (b) issuing a first security key that is indicative of limited printing resource authorization to client computers that are not members of the predetermined policy domain. These amendments find support in the specification. In particular, page 4, lines 6-14 and 25-34 provides:

> Once the use has been granted access to the various printer resources based on policy domain membership, the user is able to print to the printer and to use the printer's resources up to any limits on resource usage that are imposed. In some embodiments of the invention, limited printer resources usage may be granted to all users, with greater resource access granted to users who are members of specific policy domains. For example, a user whose computer is not located in the marketing department and who is not a member of management may be granted full access to a printer's black-and-white print capability, but have limited access to its color printing capability. (lines 6-14)
>
> In some further embodiments of the invention, the user authenticates identity to the printer by using a security or encryption key, which the printer uses to confirm identity and authorization for users. The security key is in some embodiments issued and managed by a security module within the printer, as is described in the copending patent application titled "Printer Security Key Management", filed which is hereby incorporated by reference. The security key issued to each user in such an embodiment of the invention is therefore usable not only to ensure secure communication of data between the user and a printer, but to authenticate the user's identity to the printer for granting access to printer resources. (lines 25-34)

As stated, the issued security key is useable to authenticate the user's identity to the printer for granting access to printer resources. In short, the security key is indicative of the printer resources available to a client computer. Thus, security keys issued to authenticate the user's identity would include a key granting more access to printer resources for members of the policy domain and a key granting limited access to printer resources for non-members of the policy domain.

CLAIM REJECTIONS – 35 USC §103

Claims 1-3, 13-15 and 25-27 stand rejected under 35 USC §103 as being unpatentable over USPN 6,952,280 issued to Tanimoto in view of USP Appl. Pub No. 2004/0109568 issued to Slick.

Claim 1, as amended, is directed to a printer access control module within a printer that is operable to:

1. receive a request from a client computer for printing resource authorization;
2. determine the policy domain of the requesting client computer;
3. issue a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain, wherein issuing a security key comprises issuing a first security key that is indicative of greater printing resource authorization to client computers that are members of a predetermined policy domain and issuing a second security key that is indicative of limited printing resource authorization to client computers that are not members of the predetermined policy domain; and
4. authorize a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used by the client computer to encrypt the print job.

Tanimoto, as admitted by the Examiner, does not teach the issue of "a security key to the client device or the issued security key used by the client computer to encrypt the print job." (Examiner's Response to Appellant's Opening Brief on Appeal at page 3). The Examiner then cites Slick as teaching issuing "a security key to the client device." (Examiner's Response to Appellant's Opening Brief on Appeal at page 3).

Slick recites the issuance of a single security key or key pair, where the private key is maintained within the printer and the public key is provided to users. (para. 0005) As amended, Claim 1 discusses the issuance of two security keys or key pairs. Claim 1 recites:

1. issuing a security key that is indicative of greater printing resources authorization to client computers that are members of a predetermined policy domain; and
2. issuing a security key that is indicative of limited printing resource authorization to client computers that are not members of the predetermined policy domain.

Thus, as amended, Claim 1 clearly recites a printer access control module which is capable of issuing two different keys, one for members and one for non-members. Slick, on the other hand, recites the issuance of one key to gain access to a printer. (para. 0005). Consequently, Slick, fails to teach or suggest a printer access control module having the capabilities recited in Claim 1.

Further, Claim 1 recites that the first key is indicative of greater printing resources while the second key is indicative of limited printing resources. The limiter printing resources are logically a subset of the greater printing resources. In other words, the greater printing resources included the limiter printing resources plus others. On the other hand, Tanimoto teaches that requests from designated clients/jobs print out from designated paper supply means and print requests from non-designated clients/jobs print out on paper fed from non-designated paper supply means. (Tanimoto, Fig. 4, S27 and S26) Tanimoto teaches a separation of printer resources for designated clients/jobs and non-designated clients/jobs. A print request from a designated client or job will use the

designated paper cassette or manual feed tray while a print request from a non-designated client or job will use a paper cassette or manual feed tray not dedicated to the designated client or designated job. (Tanimoto, column 4, lines 36-46) Accordingly, and as illustrated in Fig. 4, non-designated clients/jobs use a different set of resources than designated clients/jobs.

As amended, Claim 1 recites greater printing resources for policy domain members than for non-members (i.e. designated clients and non-designated clients). Claim 1 is differentiated form Tanimoto because greater printing resources available to members do not exclude resources available to non-members. There is no separate set of the resources available to non-members only. (pg 4, lines 6-14) Each member is only limited by what resources they may use based on their policy domain membership. (pg 4, line 6-7) Each member is "able to print to the printer and to use the printer's resources up to any limits on resource usage that are imposed." (pg 4, lines 7-8). Thus, an example of a difference between a member and non-member may be that a member can use resources to print in black-and-white from tray 1 and print in color from tray 2, while a non-member may only be able to print in black-and-white from tray 1. Both members and non-members have access to tray 1.

Therefore, Tanimoto even when combined with Slick fails to teach or suggest a printer access control module within a printer that is operable to authorize a print job received from the client computer to be printed using one or more printer resources indicated by one of two issued security keys, that are used to encrypt a print job. For at least these reasons amended Claim 1 and Claims 2-9 which depend from Claim 1 are patentable over the cited art.

Claim 13, as amended is directed to a printer that is operable to:

1. receive a request from a client computer for printing resource authorization;
2. determine the policy domain of the requesting client computer;

3. issue a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain, wherein issuing a security key comprises issuing a security key that is indicative of greater printing resource authorization to client computers that are members of a predetermined policy domain and issuing a security key that is indicative of limited printing resource authorization to client computers that are not members of the predetermined policy domain; and
4. authorize a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used to encrypt the print job.

As with Claim 1, neither Tanimoto nor Slick , individually or combined, teaches or suggests a printer that is operable to authorize a print job received from the client computer to be printed using one or more printer resources indicated by the issued by one of two security keys used to encrypt the print job. For at least the same reasons Claim 1 is patentable, so are amended Claim 13 and Claims 14-21 which depend from Claim 13.

Claim 25, as amended is directed to a machine-readable medium with instructions stored thereon, the instructions when executed on a computerized system operable to cause the system to:

1. receive a request from a client computer for printing resource authorization;
2. determine the policy domain of the requesting client computer;
3. issue a security key to the client device, the security key indicative of one or more printer resources available to client computers of the determined policy domain, wherein issuing a security key comprises issuing a security key that is indicative of greater printing resource

authorization to client computers that are members of a predetermined policy domain and issuing a security key that is indicative of limited printing resource authorization to client computers that are not members of the predetermined policy domain; and

4. authorize a print job received from the client computer to be printed using one or more printer resources indicated by the issued security key used to encrypt the print job.

As with Claim 1, neither Tanimoto nor Slick , individually or combined, teaches or suggests authorizing a print job received from the client computer to be printed using one or more printer resources indicated by one of two issued security keys used to encrypt the print job. For at least the same reasons Claim 1 is patentable, so are amended Claim 25 and Claims 26-33 which depend from Claim 25.

Claims 4-8, 16-19, and 28-31 stand rejected under 35 USC §103 as being unpatentable over USPN 6,952,280 issued to Tanimoto in view of USP Appl. Pub No. 2004/0109568 issued to Slick and further in view of USPN 6,490,049 issued to Cunnagin. Claims 4-8 depend from amended Claim 1. Claims 16-19 depend from amended Claim 13. Claims 28-31 depend from amended Claim 25. For at least the same reasons Claims 1, 13, and 25 are patentable so are Claims 4-8, 16-19, and 28-31.

Claim 8, 9, 20, 21, 32, and 33 stand rejected under 35 USC §103 as being unpatentable over USPN 6,952,280 issued to Tanimoto in view of USP Appl. Pub No. 2004/0109568 issued to Slick and further in view of USPN 6,545,767 issued to Kuroyanagi.Claims 8-9 depend from amended Claim 1. Claims 20-21 depend from amended Claim 13. Claims 32-33 depend from amended Claim 25. For at least the same reasons Claims 1, 13, and 25 are patentable so are Claims 8-9, 20-21, and 32-33.

Conclusion

In view of the foregoing remarks and amendments, Applicant respectfully submits that Claims 1-9, 13-21, and 25-33 define allowable subject matter. The Examiner is requested to indicate the allowability of all claims in the application and to pass the application to issue.

Respectfully submitted,
Curtis Reese

By /Jack H. McKinney/
Jack H. McKinney
Reg. No. 45,685

July 22, 2008